【人格权】

敏感个人信息的法律基准与范畴界定

——以《个人信息保护法》第28条第1款为中心

宁 园

【摘 要】《个人信息保护法》第28条第1款中敏感个人信息的“敏感”是指法律规制的高反应度,其以信息处理的权益侵害风险为法律基准,风险内容指向除个人信息权益之外的人格尊严和人身、财产权利,风险程度则以达到“一般权益侵害程度+更高风险兑现概率”为必要。敏感个人信息的界定应采取场景抽离和场景融入双重路径。场景抽离关注作为内因的信息内容,内容具有强工具性和唯一识别性的个人信息为敏感个人信息;场景融入关注作为外因的场景要素,信息处理者的认知能力、信息应用能力及信息存在状态是改变信息内容属性的主要场景要素,可以促成敏感个人信息的转化。因未成年人信息控制能力弱、信息暴露程度高,立法将其个人信息归入敏感个人信息具有合理性。第28条第1款列举的各项信息具有涵括性,不能直接作为敏感个人信息的认定依据,是否属于敏感个人信息仍须进行具体判定。

【关 键 词】敏感个人信息;风险维度;场景抽离;场景融入;强工具性;唯一识别性

【作者简介】宁园,中国人民大学法学院讲师,法学博士。

【原文出处】《比较法研究》(京),2021.5.33~49

【基金项目】本文系中国博士后科学基金特别资助项目“企业数据利益的私法保护”(编号:2021T140721)、中国博士后科学基金面上资助项目“数据治理的私法之道:概念重构、路径整合和规则构建”(编号:2020M680794)的阶段性成果。

一、问题的提出

相比于非敏感个人信息而言,敏感个人信息的泄露和非法使用更易导致权益侵害的发生,因此,域内外立法均对敏感个人信息的处理作出更为严格的限制。[①]《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)第二章第二节就敏感个人信息的处理规则进行了专门规定,具体内容包括:敏感个人信息的处理以一般禁止为原则,对其处理必须具有特定目的和充分必要性(第28条第2款);敏感个人信息处理必须取得单独同意或者书面同意(第29条);敏感个人信息处理者须承担更严格的告知义务(第30条);处理未成年人个人信息须取得其父母或其他监护人的同意,且应制定专门保护规则(第31条);敏感个人信息处理活动应当遵守其他法律、行政法规的特殊限制(第32条)。

特殊处理规则的适用前提是完成敏感个人信息的界定,《个人信息保护法》第28条第1款规定:“敏感个人信息是一旦泄露或者非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息,包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信

息，以及不满十四周岁未成年人的个人信息。”该款规定明确了敏感个人信息的法律基准为客观权益侵害风险，回应了学界有关“敏感”到底是以个体主观反应为基准，[②]还是以客观权益侵害风险为基准的争议，[③]具有重要的进步意义。然而，《个人信息保护法》第28条第1款对敏感个人信息的一般表述仍然较为笼统，各列举项也极具涵括性，其与一般表述之间的逻辑对应有待揭示。

本文认为，敏感个人信息的界定须经历三个递进阶段，一是确定敏感个人信息的法律基准，二是确定法律基准的具体维度，三是确定敏感个人信息的具体判定标准。第一阶段解决敏感个人信息的法律语境切换，即“敏感”的法律化问题；第二阶段确定权益侵害风险基准的具体维度，即什么程度的风险才符合敏感个人信息的风险基准；第三阶段确定敏感个人信息的判定标准，即确定个人信息满足何种特性时才达到敏感所要求的风险基准。《个人信息保护法》第28条第1款明确了敏感个人信息的法律基准，并在概念表述中提及了敏感个人信息的风险维度，但仍然存在以下两方面的问题：一是未充分明确敏感个人信息风险基准的具体维度，有必要作进一步解释；二是敏感个人信息的具体判定标准不明，学界有关判定标准的探讨也还停留在风险描述层面，存在风险基准和判定标准的混同，[④]故有必要予以阐明。

综上，有必要在《个人信息保护法》第28条第1款的基础上，对敏感个人信息的法律基准和范畴界定进行解释说明。下文将围绕敏感个人信息的法律基准、风险维度作进一步分析，并在优化界定路径后提出敏感个人信息的具体判定标准，以期实现敏感个人信息概念的再厘清。

二、敏感个人信息的法律基准

《个人信息保护法》第28条第1款对敏感个人信息所作的一般表述，完成了“敏感”的法律语境切换，确定了敏感个人信息的法律基准，并从风险内容、风险程度、风险发生方式三个维度完成法律基准的填充。下文将逐一进行分析，以期呈现立法者所描绘的敏感个人信息基本样态。

(一)“敏感”的法律语境切换——法律规制的高反应度

“敏感”一词在日常用语中带有主观色彩，因此，有学者将个体的主观反应度作为“敏感”的法律基准，认为法律语境下的敏感个人信息就是使人敏感的个人信息、[⑤]用户真正关心的个人信息。[⑥]此种解读以个体主观因素作为“敏感”的法律基准，是语境切换不足的结果。从个体视角来看，“敏感”一词是对该个体心理特征的描述，指个人对某种事物、现象等表现出高反应度。心理学上所探讨的敏感度，受先天基因、成长环境和社会经验的影响，有很强的个体差异性。[⑦]如有着“感觉加工敏感”(sensory processing sensitivity)特质的“高敏感人群”(highly sensitive person)的感知阈值低、认知程度深，对外界刺激表现出更高的反应水平。[⑧]若将“敏感”的心理学含义不作转化地移植于法学语境中，敏感个人信息则指个人对该信息处理表现出高反应度的个人信息(即“使人敏感的个人信息”)。显然，建立在个体主观反应基准上的敏感个人信息，范畴则完全由个人决定，立法不可能以此为基准划定确定的范畴，并将其作为信息处理的规制基础。

本文认为，法律视角下，敏感个人信息不是“使人敏感的个人信息”，敏感也并非个体心理特征，而是指法律规制的高反应度。这一点可以从《个人信息保护法》有关敏感个人信息的立法逻辑和目的中得到印证：正是因为敏感个人信息处理更易导致人身、财产权益受侵害，处理规则才更为严格，敏感个人信息处理也就更易触发法律规制，前者为规则本身的敏感性，后者为规则启动的敏感性，二者相互统一。因此，《个人信息保护法》剥离了“敏感”界定的个体主观心理因素，完成了“敏

感”的法律化。“敏感”不以主观心理敏感度为基准,而是指向法律规制的高反应度,确保了敏感个人信息作为法律概念的基本确定性。值得一提的是,日本《个人信息保护法》中的“需要特殊保护的个人信息”基本与我国“敏感个人信息”概念一致,这也在一定程度上揭示了“敏感”与法律规制高反应度之间的一致性。[9]

(二)敏感个人信息的法律基准——权益侵害风险基准

当然,并非所有受到法律特殊保护的个人信息均为敏感个人信息,“敏感”有其特殊的法律基准,即权益侵害风险基准。从文义解释来看,“敏感”对应的是“容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害”。首先,表述使用“容易导致”而非“导致”或“必然导致”,意味着“敏感”与侵害风险对应,不要求侵害必然发生。此种理解亦符合个人信息保护的风险防御功能,敏感个人信息作为特殊的个人信息,对风险进行特殊防御,其法律基准亦为风险基准。[10]其次,“人格尊严受到侵害”“人身、财产安全受到危害”表明风险指向人格尊严和人身、财产权利。需要说明的是,此处“受到侵害”与“受到危害”的表述并无实质区别。权益侵害既包括已经造成损害的情形,还包括危及人身、财产安全但还未造成现实损害后果的情形。[11]“侵害”与“危害”均指正在危及或者已经造成现实损害,二者均为法定的侵权形式。[12]

结合来看,敏感个人信息之所以促使法律规制高度敏感,乃是因为敏感个人信息具有权益侵害风险,敏感的法律基准为权益侵害风险基准,此处的“权益”既包括权利,也包括尚未权利化的法律保护的利益。权益侵害风险的法律基准在我国《信息安全技术个人信息安全规范》亦有体现,其将敏感个人信息界定为“一旦泄露、非法提供或滥用可能危害人身和财产安全,极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息”。[13]

还须说明的是,敏感个人信息的客观权益侵害风险基准使其区别于私密信息。《中华人民共和国民法典》(以下简称《民法典》)将个人信息区分为私密信息和非私密信息,私密信息属于隐私,优先适用隐私权保护规则,非私密信息则适用个人信息处理规则。[14]作为隐私的一种,私密信息须具有秘密性和私人性,秘密性即个人不愿其信息为人所知,且此种期待合理;私人性即信息保持私密不会影响公共利益、他人利益。[15]由于受个人公开意愿的影响,私密信息范畴具有主观性。[16]而敏感个人信息采客观的权益侵害风险基准,只有信息处理产生更高权益侵害风险才属于敏感个人信息。因此,敏感个人信息与私密信息仅存在交叉关系:私密信息不一定属于敏感个人信息,如个人不愿公开的考试成绩属于私密信息,但不符合敏感个人信息的风险基准;敏感个人信息也不一定属于私密信息,如特定身份属于敏感个人信息,但却不一定具有私密性;私密信息达到敏感所要求的风险基准时,二者发生重叠,如个人不愿透露的身份信息、行动轨迹等,既是私密信息,也是敏感个人信息。[17]

(三)权益侵害风险基准的具体维度

权益侵害风险在个人信息处理活动中普遍存在,并非敏感个人信息所独有,因此,敏感个人信息的界定还须明确风险基准的具体维度,以完成与非敏感个人信息的界分。从文义来看,《个人信息保护法》第28条第1款对敏感个人信息的一般表述中包含风险内容、风险程度、风险发生方式三个维度,但各维度还须进行再解释。

1.风险内容

敏感个人信息的风险内容乃风险指向的权益内容,即信息处理可能造成哪些个人权益受到侵害。在风险内容上,目前存在隐私权受侵害标准、

平等权受侵害标准(即“歧视标准”)、人身和财产权利受侵害标准。隐私权受侵害标准即认为敏感个人信息的敏感性在于其处理易导致隐私权受到侵害,敏感个人信息界定之核心标准为信息内容与隐私的关联程度。[18]平等权受侵害标准认为敏感个人信息的处理风险在于可能导致歧视。[19]人身和财产权利受侵害标准则认为敏感个人信息的处理风险在于可能导致人身、财产权利侵害的发生。[20]《个人信息保护法》第28条第1款,则将风险内容指向人格尊严和人身、财产安全。

首先,《个人信息保护法》第28条第1款并未采用隐私权标准。摈弃单独的隐私权标准具有合理性,其原因在于,个人信息安全风险并不仅仅指向隐私权,人格平等、人身自由、生命权、名誉权、财产权等诸多权利同样在信息泄露和滥用中面临风险。算法歧视、算法操控现象屡见不鲜,[21]信息泄露引发的财产诈骗司空见惯。[22]基于权利平等保护的价值理念,当上述人格权和财产权面临高侵害风险时,应当与隐私权一样获得平等的法律保护。这也是风险内容不应局限于某些特定权利的原因。此外,单采隐私权标准,是将敏感个人信息等同于私密信息,不仅与《个人信息保护法》设置敏感个人信息分类的立法目的相左,且与立法所确立的敏感个人信息客观风险基准相悖。

其次,《个人信息保护法》第28条第1款所述的“人格尊严”和“人身、财产安全”也不应局限为所谓“重大权利”。原因在于,所谓“重大权利”并非法定的权利类型,将风险内容限制为“重大权利”,只会引起处理规则的适用混乱。如按权利位阶排序,人格权位阶高于财产权,但若按损害后果的严重性排序,通常认为财产权比姓名权、肖像权等人格权更为重要,因此,“重大权利”并不存在确定标准和范围,以此作为风险内容维度无益于敏感个人信息的界定,反而阻碍其发挥确定的指引作用。

本文认为,《个人信息保护法》第28条第1款实际采用了广泛的人身、财产权益标准,对敏感个人信息的风险内容基本不作限制(个人信息权益除外),凡是容易因敏感个人信息泄露、非法使用受到侵害的权利或者利益,均属于敏感个人信息的风险内容。条文中的“人身、财产安全”指向人身、财产权利,“人格尊严”则为敏感个人信息处理可能造成的尚未权利化的利益侵害兜底。

具体而言,“人身、财产安全”是指“人身、财产权利的安全”“人身、财产权利不受侵害”,因此,风险内容包含人身、财产权利。此处的人身、财产权利包括生命权、身体权、健康权、姓名权、肖像权、名誉权、荣誉权、物权、债权等广泛的个人权利类型,但一般人格权和个人信息权益除外。其原因在于,首先,一般人格权由《个人信息保护法》第28条第1款的“人格尊严”所涵括,故为避免重复,不包含在人身、财产安全所指向的人身、财产权利范畴内。其次,敏感个人信息的风险内容不应包含个人信息权益本身。将个人信息权益侵害纳入风险内容存在“倒果为因”的逻辑错误。正是由于一项个人信息属于敏感个人信息,应适用更为严格的处理规则,个人信息侵权要件才更易被触发。可见,个人信息权益侵害风险高低实际上以完成敏感个人信息界定为前提,不应反过来成为敏感个人信息界定的风险基准。

“人格尊严”所指向的风险内容则是尚未权利化但同样应受法律保护的其他人格权益,其作为一般人格权发挥兜底保护作用。我国民法典第990条乃人格权保护的一般规定,其第1款列举了法律保护的具体人格权,第2款为一般人格权条款,规定基于人身自由、人格尊严产生的其他人格权益亦受法律保护。人身自由、人格尊严作为一般人格权产生的价值基础,是立法者为应对新型人格权益侵害、避免具体人格权保护漏洞所设置

的兜底保护条款。[23]《个人信息保护法》第28条第1款将人格尊严侵害纳入风险内容，意在通过人格尊严的一般人格权地位，将一旦泄露或者非法使用容易导致其他人格权益侵害的个人信息纳入敏感个人信息范畴，以扩充敏感个人信息处理规则所保护的权益范围。此一目的从《中华人民共和国个人信息保护法(草案二次审议稿)》(以下简称《个人信息保护法(草案二审稿)》)到《个人信息保护法》的立法流变也可以看出，《个人信息保护法(草案二审稿)》第29条第2款所规定的风险内容为“受到歧视”与“人身、财产安全受到严重危害”，《个人信息保护法》第28条第1款直接将“受到歧视”改为“人格尊严受到侵害”，以侵害人格尊严代替受到歧视，既囊括歧视所指向的人格平等，又进一步扩展了风险指向的权益内容，以应对个人信息处理中尚未权利化的和新型的利益侵害风险。此外，将人格尊严置于人身、财产安全之前，也与个人信息保护的根本出发点——人格尊严保护——相呼应。

当然，此处仅列举人格尊严，并不包含《民法典》第990条第2款所规定的人身自由。本文认为，尽管《民法典》将一般人格权的派生基础规定为人身自由、人格尊严，但从解释上来讲，人格尊严是相比于人身自由而言更为基础的价值，尊重个人的身体行动自由和自主决定的自由，也是人格尊严的应有内容。[24]因此，《个人信息保护法》第28条第1款中的“人格尊严”可解释为包含人身自由，与以人身自由、人格尊严为价值基础的其他人格权益等同。

综上，敏感个人信息安全风险内容指向除个人信息权益之外的人身、财产权利和以人格尊严为价值基础的其他人格权益，并不局限于隐私权和所谓的“重大权利”。可见，在风险内容上，敏感个人信息与非敏感个人信息并无不同，二者的区别主要体现在风险程度上。

2.风险程度

敏感个人信息的风险程度包含两个方面：一是权益侵害程度，即作为敏感个人信息的权益侵害须达到何种程度；二是风险概率，即权益侵害风险的兑现概率。《个人信息保护法》第28条第1款表示权益侵害程度的是人格尊严“受到侵害”和人身、财产安全“受到危害”；表示风险兑现概率的是“容易导致”。依文义解释，该款对风险程度采取统一的“一般权益侵害程度+更高风险兑现概率”标准，相比于《个人信息保护法(草案二审稿)》区分歧视和人身、财产侵害，并分别采取“一般权益侵害程度+无差别风险兑现概率”和“严重权益侵害程度+无差别风险概率”的做法，[25]更能清晰体现敏感个人信息法律特性，构建科学合理的个人信息分类体系。

首先，从文义来看，《个人信息保护法》第28条第1款将《个人信息保护法(草案二审稿)》中的“人身、财产安全受到严重危害”改为“人身、财产安全受到危害”，删除“严重”一词，对敏感个人信息处理风险的权益侵害程度统一采一般侵害程度，即敏感个人信息所要求的风险只是人格尊严和人身、财产权利受侵害的风险，并不是权益受到严重侵害的风险。此一修改具有合理性。其理据在于，要求风险达到严重危害权益的程度，不仅无益于敏感个人信息范畴的划定，且会产生不平等的差别保护，破坏处理规则的规制作用。具体而言，一是，权益侵害程度是否严重与信息敏感与否关系甚微。权益侵害后果严重与否，更多是受被侵害的权利内容(如侵害生命权还是财产权)、受害人具体状况、行为人的侵权手段等因素的影响，与信息敏感与否关联度低。如因电话号码泄露引发的电信诈骗可能给受害人造成巨额财产损失，也可能仅对信息主体造成叨扰，这与信息主体的自我保护意识、社会经验、经济状况以及行为人的诱导能力、欺骗手段等关系更为密切。因此，引入与

敏感关系甚微的“严重”一词,无益于敏感个人信息范畴的划定。二是,要求侵害达到严重程度,会造成不平等的差别保护。如由于经济实力差异,富人账户信息泄露造成的财产损失重于穷人,更易达到严重程度之要求,由此造成的后果是,只有富人的账户信息才属于敏感个人信息,受到更高程度的保护,这显然与平等原则相悖。三是,从我国立法和司法实践可以看出,危害严重与否是对损害后果进行事后的、确切的判定,预测性弱,不应将其作为指引规则适用的概念之界定标准。如在涉及侵害身体权、健康权的精神损害赔偿案件中,法官往往以损害后果达到何种伤残等级来判断损害后果是否达到严重程度。[26]又如《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》对侵犯公民个人信息罪之情节严重的认定多以具体的危害结果作为标准,如“非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的”、“非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的”。[27]可见,要求侵害达到严重程度,会导致敏感个人信息沦为事后概念,瓦解处理规则的防御规制意义。

其次,《个人信息保护法》第28条第1款对敏感个人信息处理风险的兑现概率采高于非敏感个人信息的“更高风险概率”。[28]从文义上来看,该款将《个人信息保护法(草案二审稿)》的“可能导致”改为“容易导致”。从“可能”到“容易”,立法者显然对敏感个人信息的风险兑现概率作了更高要求。至于这一更高要求的标准何在?本文认为,应以高于非敏感个人信息之风险兑现概率为必要。“容易”应解释为相对于非敏感个人信息而言,敏感个人信息处理须更可能侵害人格尊严和人身、财产权利。其原因在于,在数据技术高度发达的今天,任何个人信息处理都存在权益侵害风险;且随着技术的逐渐成熟,风险形式从传统的识别型侵害风险向歧视型、控制型侵害风险扩散,风险波及的权利范围也随之扩张。在风险内容上,非敏感个人信息与敏感个人信息并无差异。若不对敏感个人信息的风险兑现概率作更高限制,则难以区分敏感个人信息与非敏感个人信息。要求敏感个人信息存在更高风险兑现概率,明确敏感个人信息与非敏感个人信息的根本区别,既有助于构建清晰的个人信息分类体系,又明确了敏感个人信息受到特殊保护的根本原因:某些个人信息之所以“敏感”,是由于此类信息处理更可能被用于违法行为、导致权益侵害,因而需要法律特殊规制。因此,敏感个人信息之风险程度的特殊性凸显于其风险兑现概率,风险程度为“一般权益侵害程度+更高风险兑现概率”,不同于非敏感个人信息的“一般权益侵害程度+无差别风险兑现概率”。

3.风险发生方式

《个人信息保护法》第28条第1款将敏感个人信息的风险发生方式区分为泄露和非法使用,分别对应泄露型风险和非法使用型风险。两种风险类型的主要区别为信息作用机制的差异。泄露型风险是仅因信息泄露即被触发的权益侵害风险,典型的泄露型风险为隐私权受侵害的风险和平等权受侵害的风险(即歧视风险);非法使用型风险则主要是利用信息、以信息作为行为控制工具时引发的权益侵害风险,其风险内容范畴更广,包括生命权、身体权、健康权、隐私权等人格权受侵害的风险和财产权受侵害的风险。

前文对敏感个人信息的法律基准及其维度进行了系统分析,主要内容总结于下表1。

三、敏感个人信息的双重界定路径

敏感个人信息权益侵害风险基准和风险维度的明确,一定程度上明晰了敏感个人信息的范畴,但仍面临挑战:如何判定个人信息泄露或非法使

表1 敏感个人信息权益侵害风险基准的三个维度

	具体维度	《个人信息保护法(草案二审稿)》	《个人信息保护法》
权益侵害风险基准	风险内容	人格平等(歧视标准)以及人身、财产权利	人身、财产权利以及人格尊严派生的其他人格权益
	风险程度(侵害程度、风险兑现概率)	(1)人身、财产权利:严重侵害程度+无差别风险兑现概率;(2)歧视:一般侵害程度+无差别风险兑现概率	统一的一般权益侵害程度+更高风险兑现概率
	风险发生方式	泄露型风险和非法使用型风险	泄露型风险和非法使用型风险

用的风险达到敏感的风险维度?《个人信息保护法》第28条第1款并未涉及判定标准,有必要予以明确。为实现这一目标,不少学者提出敏感个人信息的场景化界定方案,主张在具体场景中完成敏感个人信息的界定。[29]场景融入路径有其合理性,但其忽视了风险发生的内因,不能独立完成敏感个人信息的界定。本文认为,敏感个人信息的界定应并用场景抽离和场景融入路径。

(一)场景融入路径的局限性

场景融入路径,即在个人信息处理的具体场景中界定该个人信息处理风险是否达到敏感个人信息处理的风险基准。国内场景融入方法主要是受到美国学者尼森鲍姆(Nissenbaum)"场景完整性理论"(contextual integrity)的启发。为应对信息技术带来的隐私保护挑战,场景完整性理论将隐私保护与具体场景相关联,将隐私权是否受到保护转变为个人信息披露和流通是否符合特定场景的合理性规范和信息流通规范问题。[30]以场景融入的路径界定敏感个人信息,继受了场景完整性理论的内在理念,主张在具体场景中考量个人信息处理风险大小,以解决敏感个人信息的动态界定问题。场景融入有助于提供更为确定的风险评估环境,缓解敏感个人信息界定的不确定性,有其必要性。然而,场景融入路径亦存在如下两方面缺陷:一是,场景融入路径是对敏感个人信息范畴的不确定性进行被动消化,敏感个人信息只能在特定场景下即时确定。在此被动模式之下,敏感个人信息范畴多随场景变动,只能成为事后救济是否启动的标准,处理规则的预防功能难以实现。二是,单一场景融入路径仍然无法解决敏感个人信息的界定问题,一项个人信息是否为敏感个人信息,仍须在具体的场景中寻求更为根本恒定的认定标准,场景始终只是影响个人信息处理风险的外因,穿透场景寻求内因才是敏感个人信息界定的终极方案。[31]因此,仅靠场景融入路径,无法完成敏感个人信息范畴的划定。

(二)双重路径——场景抽离与场景融入并用

基于场景融入路径的局限性,本文提出场景抽离路径,具体包括场景预先剥离和场景穿透两种形式,一是通过场景预先剥离构筑敏感个人信息的先在确定范畴,即抽离具体的、特定的场景,只关注哪些信息在其绝大多数处理场景中具有更高的权益侵害风险,这类敏感个人信息始终适用特殊处理规则,无论具体处理场景为何;二是场景穿透,是在融入场景后,穿透场景寻求敏感个人信息的根本认定标准,这类敏感个人信息仅在该特场景下适用特殊处理规则。二者的区别在于,前者不预设个人信息处理的特定场景,是在具体场景发生前而非发生时预判个人信息处理风险,以实现敏感个人信息的先在界定;[32]后者是在特定场

景发生之后，再进行场景穿透，探寻场景这一外部作用机制所引发的内因变动，以完成敏感个人信息的界定。无论是场景预先剥离还是场景穿透，均关注影响个人信息处理风险的内因，其本质是通过判断信息内容是否足以独立地或者在场景刺激下引发更高的权益侵害风险来界定敏感个人信息。

敏感个人信息界定并用场景抽离路径和场景融入路径有其必要性。

首先，从敏感个人信息处理制度的功能实现来看，场景抽离与场景融入的结合具有必要性。为实现敏感个人信息的预防保护和周全救济，敏感个人信息界定须同时发挥先在指引功能和动态矫正功能，全面保护和双重功能的实现以场景预先剥离和场景融入的并用为必要。

在敏感个人信息保护体系中，预防手段最为契合其防范多元权益侵害风险的目的，[33]无论是欧盟《通用数据保护条例》、日本《个人信息保护法》，还是我国《信息安全技术个人信息安全规范》以及《个人信息保护法》，均将预防保护作为风险控制的关键，在规则设置上纷纷提高处理门槛、严格告知同意要件以在信息处理之前尽量降低侵害风险。[34]因此，敏感个人信息的界定必须为预防保护的实现留有空间，其指引不仅仅是确定的指引，还须包括先在的指引。先在指引功能要求敏感个人信息范畴具有先在的确定性，单纯强调场景融入路径很大程度上妨碍了此项功能的发挥。因此，通过场景预先剥离，挖掘不受具体场景左右的敏感个人信息的先在确定范畴，有助于构建完整的敏感个人信息概念体系，充实处理规则的规制层次，更好地应对复杂的敏感个人信息处理实践。

当然，为弥补先在确定范畴封闭僵化造成的保护漏洞，敏感个人信息概念还须发挥动态矫正功能，将未纳入先在确定范畴但又在特定场景下转化为敏感个人信息的信息纳入特殊规制范围内。场景融入路径则是周全保护敏感个人信息的动态策略，其保持了敏感个人信息范畴的弹性，确保事实上的敏感个人信息得到法律特殊保护。因此，场景预先剥离和场景融入的结合有助于实现敏感个人信息概念确定性与灵活性的平衡，发挥处理规则的周全保护作用。

从个人信息处理风险的影响因素来看，场景抽离和场景融入的结合具有必要性。个人信息处理风险同时受信息内容和其所处场景两方面的影响。内容是个人信息承载利益、与他人和社会发生联结的基点，也是侵害风险存在的基础，信息无内容就无法与个人和社会产生互动，风险亦不存在。信息处理风险的产生归因于信息内容的泄露或非法使用。因此，内容是风险产生的内因。场景则通过改变信息内容的属性影响信息处理风险。在信息内容被充分解析利用的场景中，其风险也更高，而在信息内容未被理解和利用场景中，风险也就保持在低水平。以基因序列为例，[35]基因序列信息的理解和利用需要在医学、生物学等专业场景中实现，于常人来说则并非易事。因此，基因序列信息敏感度在一般社会场景中远低于专业场景(如科学研究)，后一场景中基因序列信息的滥用风险大大提高。从内容和场景的作用来看，基因序列信息内容本身是风险发生的根源和内因，场景变化改变内容的可理解、可利用属性，进而改变风险程度。因此，即使在场景融入路径下，风险评估仍须回归信息内容本身，通过探寻场景引起的信息内容变动，认定敏感个人信息。

可见，内容是风险产生和存在的内因，场景是作用于内容属性从而改变风险程度的外因。敏感个人信息的界定应当同时考量内容要素和场景要素两个方面，前者关注当个人信息内容具有哪些属性时风险达到敏感基准，须通过场景抽离路径实现；后者关注哪些场景要素足以改变以及如何改变个人信息内容属性，使其处理存在更高风险，

须通过场景融入路径实现。

总之,场景抽离与场景融入在敏感个人信息的界定中互为辅助,场景预先剥离与场景融入的结合有助于构建先在确定和即时确定的敏感个人信息的完整范畴,最大程度地发挥相关处理规则的规制作用;场景融入路径最终必然导向场景穿透,场景要素如何触发个人信息处理风险,仍须审查其对信息内容属性的影响。

四、敏感个人信息的判定标准

(一)场景抽离——回归作为内因的信息内容

场景抽离路径意在使敏感个人信息的界定脱离或穿透某一具体场景的限制,回归信息内容本身,探讨风险存在和发生的内因。在场景预先剥离语境下,信息内容本身就酝酿更高的权益侵害风险,无须场景作为额外触发机制;在场景穿透语境下,场景要素改变信息内容,使其具备触发高风险的特有属性。因此,敏感个人信息的判定标准最终指向易引发权益侵害的信息内容属性。本文认为,具有强工具性和唯一识别性的个人信息为敏感个人信息。

1.强工具性

信息内容的工具性越强,越易引发权益侵害风险,尤其是非法使用型风险。欲论证此观点,首先须释明信息与行为之间的本质关联。在认识论范畴上,信息是主体与物质间的相互作用,其存在于个人对外界的感知和辨认中,具有属人性。[36]信息活动本质上是认识活动,其与实践之间存在密切联系。一方面,信息只有以行为控制为目的,才有被认识的需要,才有可能成为信息。[37]另一方面,主体在实践中都是"以信息方式具身的有机体",[38]主体行为和决策伴随信息的获取和传递,社会关系发生的过程是信息互相连接、嵌入的过程。行为和决策以信息为必要,主体获取信息目的在于实现和保障行为控制。[39]社会经验也传达着信息在行为决策中的重要性:掌握充足信息的主体往往更易在博弈中占得优势。

信息是行为控制的必要工具,其有助于科学决策,但也可能被作为侵权、犯罪和其他违法行为的实施工具。大量因个人信息滥用引发的违法行为印证了这一点:诈骗、以他人名义办理信用卡、冒名顶替上学等皆以获取受害人充足的个人信息为前提。可以说,信息安全风险之所以前所未有,与"信息爆炸"导致信息作为工具的可得性大大提高密不可分,其客观上刺激了违法意图的滋生,降低了违法行为的实施难度。

信息普遍存在工具性,但在工具性的强度上存在差异。例如,身高信息的工具性显然弱于姓名,前者作为描述性信息,多仅用于向他人展示个人特质,后者则是个人在社会关系中标识和表征自己的符号,充当着最为基本的社交工具。应当认为,相比于非敏感个人信息,敏感个人信息的内容须具有强工具性,其高度可利用的特性在刺激恶意滋生、降低侵害难度等方面作用明显,客观上增加了违法行为主体数量、违法行为方式和违法行为发生概率。至于敏感个人信息的强工具性如何判定,本文认为须从信息内容是否易于认知、是否具有强中介作用两个维度考量。

(1)易于认知

个人信息的强工具性以其内容易于认知为必要条件。强工具性直接表现为高度可利用性。利用以认知为基础,因此,信息内容易于认知是衡量强工具性的标准之一。易于认知描述的是个人信息内容可被信息处理者理解的特性。易于认知的特性并不排斥技术处理,那些广泛应用于社会生活且与信息高度结合的技术(如指纹识别技术、面部识别技术),已经内化为信息易于认知的基础。个人信息内容是否易于认知主要受到两个因素的影响:一是内容本身是否超出信息处理者的认知能力;二是内容表现形式是否超出信息处理者的认知能力。若信息内容本身处于信息处理者的认

知盲区或需要信息处理者额外耗费巨大精力才能习得,其通常难以被用于控制行为;若信息形式超出信息处理者的认知能力,信息内容亦不易于认知,如由0和1组成的代码对于不掌握代码知识和数据技术的普通个人而言就难以理解。因此,作为敏感个人信息的内容必须同时在表现形式和内容上易于认知,难以被信息处理者所认知的个人信息由于工具性弱,不应被界定为敏感个人信息。必须强调的是,在场景预先剥离路径之下,先在确定的敏感个人信息,必须是信息内容和信息形式能被普遍认知的信息,如身份证号码。除此之外,易于认知性则受场景影响,须在场景中作具体判定。

(2)强中介作用

个人信息的强工具性还须以信息内容的强中介作用为要件。易于认知是信息内容具备强工具性的必要非充分条件,易于理解而难以为信息处理者利用的个人信息广泛存在,如某个人的身高、兴趣爱好之于一般人而言,并无用处。因此,信息内容的强工具性还须以信息具有强中介作用为必要。

信息可以作为联结主观世界和客观世界的中介,其中介作用体现为两个层次:一是客观世界通过信息传递改变主观认知,二是将已认知的信息用于改造客观物质世界。[40]上述关于信息中介作用的哲学描述在个人信息利用中则体现为主体获取个人信息和将该个人信息用于行为控制两个阶段。第一层次的中介作用涉及前文讨论的易于认知性,此处所说的强中介作用则是指第二层次的中介作用,即可用于改造客观世界、作用于他人的属性。不同信息在中介作用上存在区别,如身份证号码相比于个人的身高、职业等描述性信息,[41]显然在个人行为中发挥更为显著的中介作用,实践中冒用身份证也是个人信息滥用行为的"重灾区"。

强中介作用要求信息内容被必要且普遍地用于能够影响个人信息主体利益的行为中。一方面,个人在行为实施中对信息具有高度需求,即个人信息利用是行为实施的必要工具,且此种必要性普遍存在,当信息处理者在多数场景或特定场景的多数情形中均须利用某种个人信息时,该个人信息即具有强中介作用。另一方面,该信息还必须作用于影响个人信息主体利益的行为中。例如,身份证号码的强中介作用体现在:一方面,其是个人证明身份、他人验证身份的可信表征,而身份认证往往是行为实施的第一步,如在申领信用卡、注册微信账号、签订合同、办理酒店入住等场景中,均要求进行身份认证,身份证号码的中介作用在多数场景中均有体现,其使用具有普遍的必要性。另一方面,上述行为与个人信息主体利益有直接关联,如身份证一旦被他人冒用,极易导致本不应由该个人承受的法律关系归于其名下。与此类似的还有人脸信息。随着面部识别技术的推广,"刷脸"成为身份验证的又一普遍方式,酒店入住、景点游览、小区出入、银行开户等都以人脸识别为必要,人脸信息无疑也具有强中介作用。相比而言,身高的中介作用则弱得多,多数行为实施不以知晓身高信息为必要,且身高信息的可利用性弱,利用身高信息实施的影响个人信息主体利益的行为有限,权益侵害风险较小。

2.唯一识别性

敏感个人信息还应具有唯一识别性,可以用于区分出特定的个人。其原因在于,任何权益侵害的发生都有特定的受害人,而具有唯一识别性的个人信息最有助于侵害人挑选、确定受害人,也是行为人为降低侵权失败风险所极力获取的信息类型。相比于仅具有直接识别性甚至间接识别性的个人信息,唯一识别性信息是可靠的个人区分工具,具备唯一识别性的个人信息更容易导致权

益侵害发生。正因如此,唯一识别性是判断强工具性的标准之一,只有具备唯一识别性的信息才被认定为具备强工具性。

唯一识别性首先要求敏感个人信息的内容具有直接识别性而非间接识别性。仅具间接识别性的个人信息难以单独识别个人,侵权风险低,无须受特殊保护。唯一识别性其次要求敏感个人信息内容与个人一一对应,仅具有直接识别性而不具有一一对应性的个人信息亦不宜被认定为敏感个人信息,如姓名、MAC地址等。[42]这主要是基于利益平衡的考虑,敏感个人信息适用特殊保护规则,在信息收集、利用规则上受到严格限制,仅要求敏感个人信息具有直接识别性将过分抑制信息利用价值的发挥,也有损他人的自由。正是出于保护他人行为自由的考量,不具唯一识别性的姓名在各国立法例中并未被作为敏感个人信息受到特殊保护。必须注意的是,唯一识别性以区分出特定个人为已足,并不要求指明特定个人的身份。

此外,具备唯一识别性的个人信息未必具有强工具性(但仍须易于认知),但仍有可能被界定为敏感个人信息。其中典型的是,容易导致歧视的信息内容(如某人患有艾滋病的信息、有传染病史的信息等)。此类信息虽不是行为控制的必要工具,但一旦泄露易诱发偏见,导致歧视,侵害个人信息主体的人格尊严,因此应当被界定为敏感个人信息。[43]《个人信息保护法》第28条第1款所列举的宗教信仰即属此类。需要明确的是,此类信息必须是容易诱发社会偏见而非个人偏见的信息内容。其原因在于,单纯的个人偏见极具主观性,与敏感个人信息法律基准的客观性不符,且个人与遭受偏见者往往力量相当,个人偏见难以外化为歧视。而社会偏见是大众心理、文化观念、经济发展水平等社会客观因素长期积淀的结果,是社会发展形成的客观烙印,普遍存在于个人观念中,具有普遍性和客观性,且社会偏见背后往往有强大的权力支撑,[44]足以压制被歧视者的反抗力量,外化为歧视。[45]

综上所述,场景抽离路径下,当一项信息内容具有强工具性和唯一识别性时,其处理风险达到"敏感"的法律基准,应被认定为敏感个人信息。在场景预先剥离语境下,内容具有上述属性的个人信息属于先在确定的敏感个人信息;在穿透场景语境下,个人信息因场景要素获得上述内容属性才转化为敏感个人信息,属于即时确定的敏感个人信息。

(二)场景融入——触发内因的外部场景要素

非敏感个人信息在特定场景下转变为敏感个人信息,是作为外因的场景改变信息内容属性、增加风险概率的结果。一方面,信息处理风险的高低最终仍然取决于信息内容是否具有强工具性和唯一识别性;另一方面,场景促使信息内容具备敏感属性时,非敏感个人信息转化为敏感个人信息。因此,采行场景融入路径的核心在于探讨哪些场景因素可以使信息内容获得强工具性和唯一识别性。

1.信息处理者的认知能力

敏感个人信息无论是具有强工具性还是唯一识别性,都必须以易于认知为必要。在特定场景下,信息是否易于认知,主要受信息处理者的认知能力的影响。

具体而言,信息处理者的认知能力受信息处理者的主观认知能力、客观认知技术两方面的影响。就信息处理者的主观认知能力而言,当特定场景下信息处理者具有理解信息所必要的、专业的知识时,信息相对于处理者而言具有易于认知性,如掌握密码规律的信息处理者才可以轻松破译密码内容。就信息处理者的客观认知技术而言,信息处理技术越先进,信息越易被认知,如大数据技术可以读取和分析非结构化数据的具体信

息内容，非结构化数据相对于数据技术的控制者而言，即具有易于认知性。当然，在现代技术场景下，主观认知能力和客观认知技术通常同时发挥作用，信息处理者借助大数据技术和算法技术获得了强大的信息认知能力，可以快速地从诸多数据中解析信息内容。

信息处理者认知能力的改变也可能会促使信息内容隐藏的唯一识别性显现出来。若该信息的唯一识别性因难以认知而被隐匿，当信息处理者认知能力达到要求时，唯一识别性“从隐到现”的转变与信息易于认知性的形成一并发生。同样地，易于认知性的产生也可能一并呈现信息的强中介作用或社会偏见内容，从而发生非敏感个人信息向敏感个人信息的转化。

2.信息处理者的信息应用能力

信息处理者的信息应用能力影响信息的中介作用，信息处理者应用能力越强，越能充分挖掘信息的可利用价值。信息认知能力是信息应用能力的基础，前者的提升可改善后者。除此之外，应用前景开发能力是信息应用能力评估的重要考量因素。在一般情况下，可利用的信息范围和信息的可利用性受制于目的实现所需的信息范畴及信息关联度要求。因此，能够创新应用目的、降低信息关联度要求，即可实现信息应用范围和应用程度的改善，扩大具有强中介作用的个人信息范围。例如，大数据技术场景下，信息处理者的应用不再受限于已确定的目的，而是可以根据信息内容创新应用方向，且仅需信息与目的之间具有相关关系即可，此时，信息的应用方向获得极大延展，具备强中介作用的信息范畴亦相应扩张。

3.信息存在状态

信息存在的状态会影响信息内容本身和内容呈现程度，从而改变信息内容的属性。通常而言，处于单个状态的信息，内容零碎、难以理解、识别性弱、可利用性差，其权益侵害风险也低；而信息处于汇聚状态时，信息内容可通过相互联系、相互补充而充分展现，从而提高信息的可认知性、识别性和可利用性，其处理风险亦增加。因此，信息是否处于汇聚状态以及汇聚程度，是判定信息是否敏感的场景要素之一。

事实上，信息汇聚场景要素在私密信息保护的司法实践中已有应用。在庞理鹏诉中国东方航空股份有限公司、北京趣拿信息技术有限公司隐私权纠纷案中，法院在机票预订场景下将姓名、电话号码与行程信息一道认定为私密信息；法院认为，原告单独的姓名和电话号码作为社交工具不构成隐私，然而上述信息在机票预订场景中与个人的行程信息结合，完全可以与特定的个人相匹配，进而判决被告擅自收集和使用原告姓名、电话号码构成隐私权侵权。[46]此时姓名和电话号码在汇聚场景下获得私密性，转化为私密信息，受到特殊保护。非敏感个人信息因汇聚转变为敏感个人信息的认定思路与此一致。必须明确的是，在信息汇聚场景下，个人信息的敏感性是就汇聚信息整体而言的，敏感个人信息特殊保护规则的适用也仅针对汇聚的个人信息，脱离汇聚状态的个人信息，不再具有敏感性。

4.特殊场景要素——信息主体为未成年人

除上述影响信息内容属性的场景要素之外，还存在一项特殊的场景要素，同样会改变信息处理风险程度，即个人信息主体为未成年人。《个人信息保护法》第28条第1款在《个人信息保护法(草案二审稿)》基础上，将未成年人个人信息明确规定为敏感个人信息。由此，无论个人信息内容为何，只要信息主体为未成年人，均应适用敏感个人信息处理规则。

本文认为，此种立法安排是从信息主体端而非信息处理者端考察信息处理风险，其主要是出于未成年人信息控制能力弱、信息暴露程度高两

方面的考量。首先,未成年人不具备完全民事行为能力,其信息控制能力普遍较弱,极易在未充分知晓处理目的、方式、范围和风险的前提下任意授权。相比于其他信息主体而言,此类信息主体更易遭受信息泄露和非法使用,权益遭受侵害的风险也更大。其次,相比于其他不具备完全民事行为能力的个人信息主体,未成年人又是充分参与社会,尤其是信息处理集中的网络虚拟世界的"活跃分子",其信息更充分地暴露在信息处理者面前,面临更大的安全风险。因此,《个人信息保护法》将未成年人个人信息单独列为敏感个人信息的立法安排,同样是基于更高的处理风险,与立法对敏感个人信息在个人信息分类体系中的定位相匹配。

5.典型的信息转化场景——以自动化决策场景为例

自动化决策是以大数据和人工智能为技术支持的算法应用,其代替个人完成数据处理并自动生成决策,已被普遍应用于广告推送、信用评级等方面。[47]自动化决策是非敏感个人信息转化为敏感个人信息的绝佳场景。首先,自动化决策以深度学习、神经网络等数据分析技术为依托,信息处理者掌握了先进的信息分析工具和极强的信息分析能力,信息间的关联性和盖然性被广泛揭示和利用。[48]其次,自动化决策以巨量数据为决策基础,大量识别性弱的数据汇聚形成具有唯一识别性的个人信息聚合形态。因此,在自动化决策场景下,非敏感个人信息极易因分析技术先进、汇聚程度高而易于认知、利用和区分个人,从而转化为敏感个人信息,其处理风险普遍高于非自动化处理场景下的风险水平。

除了信息处理技术和信息汇聚催化处理风险外,算法错误、算法黑箱进一步加剧了自动化决策中的权益侵害风险和保护难度。因此,在立法选择和司法实践中,与费心在自动化场景之下辨别敏感个人信息相比,更明智的是将自动化决策作为特殊处理场景进行单独规制。[49]在自动化决策中,场景规制相比信息分类规制的优势在于,可以通过整体性的特殊场景规制实现敏感个人信息的高度动态保护。当然,特殊场景规制与信息分类规制并不冲突,敏感个人信息的自动化决策须同时符合敏感个人信息处理规则和自动化处理规则,但对于界定困难的个人信息,则可受到自动化决策处理规则的特殊保护,以缓解敏感个人信息转化频繁带来的跟踪规制压力。《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》的出台,即体现了依场景区分规制的思路。[50]

综上,在场景融入路径下,信息处理者的信息认知能力、信息处理者的信息应用能力、信息存在状态以及信息主体为未成年人是影响处理风险的主要场景要素。除未成年人个人信息外,在适用过程中,需要判定场景要素的样态,在融入场景之后,对内容属性进行再分析。场景融入认定的敏感个人信息具有即时性,超出此一场景则须重新考察内容属性。

五、结语:关于《个人信息保护法》第28条第1款的解释

(一)界定条款一般表述的解释

前文有关敏感个人信息的风险基准、风险维度的阐释,基本完成了对敏感个人信息界定条款一般表述的解释,总结如下:我国敏感个人信息采客观权益侵害风险标准,风险内容指向除个人信息权益之外的广泛人身、财产权益,其中"人身、财产安全"则指向人身、财产权利,"人格尊严"则指向尚未类型化的法律保护的其他人格权益;风险程度则为"一般权益侵害程度+更高风险兑现概率",风险所要求的权益侵害程度不以达到严重程度为必要,人格尊严"受到侵害"和人身、财产安全"受到危害"即可,权益侵害风险兑现概率则须达

到“容易”程度,以高于非敏感个人信息的风险兑现概率为必要;风险发生形式主要为泄露型风险和非法使用型风险。

此外,界定条款一般表述应同时包含两个范畴的敏感个人信息,即先在确定范畴和即时确定范畴。先在确定的敏感个人信息处理始终适用特殊处理规则,不受具体处理场景的影响;即时确定的敏感个人信息处理则仅在对应场景下适用特殊处理规则,其他情形则适用一般处理规则。本文认为,身份证信息、护照信息等通用的唯一身份认证信息属于先在确定的敏感个人信息,信息处理者在任何场景处理信息主体的上述信息时,都应遵循敏感个人信息处理规则。

(二)界定条款各列举项的解释

《个人信息保护法》第28条第1款在一般表述之外,明确列举生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹为敏感个人信息,并以“等”字兜底。然而,各列举项涵括性强,包含诸多具体的个人信息类型,不可一概视为敏感个人信息,适用时仍须作具体判定。

首先,各列举项所包含的个人信息并非当然属于敏感个人信息,具体判定仍须满足“敏感”的法律基准和判定标准。界定条款各列举项所涉内容广泛,并非指向某一特定信息。其中,生物识别指个人生物识别信息,包括个人基因、指纹、声纹、掌纹、耳郭、虹膜、面部特征等;宗教信仰包括是否信仰宗教、信仰何种宗教的信息;特定身份既包括身份证、军官证、护照、驾驶证等,还包括职业身份;医疗健康信息既包括个人的就诊记录、用药记录、病史、身体症状等医疗活动中产生的信息,还包括体重、心率、身高、肺活量等衡量个人健康状况的信息;金融账户信息既包括银行账户、股票账户、支付宝账户,还包括账户密码、支付口令等;行踪轨迹则包括访问地点、出行时间、出行方式等等。[51]单从文义解释来看,各列举项既涉及敏感个人信息(如身份证、传染病史等),又涉及非敏感个人信息(如身高)。因此,各列举项应视作对敏感个人信息常见类别的提示,敏感个人信息界定不能以是否属于各列举项为标准,仍须回到是否符合敏感风险基准的判定上。

其次,上述列举项并非单个状态的信息,而是指聚合状态的信息。列举类别是个人信息要义的指征,但各列举项应当解释为以此为核心要义的聚合信息群。如行踪信息并非指某一地点,而是指“信息主体去过或者将要去某一地点(甚至还包括行程时间)”这类信息群。强调各列举项处于聚合状态的原因在于,单个信息往往呈现碎片化特点,内容和利用价值均十分有限,若将列举信息解释为单个信息,则会得出一切信息均不足以单独产生权益侵害风险而不属于敏感个人信息的结论,与信息处理实践相去甚远,于司法争议处理也毫无意义。且单个信息显然不满足敏感个人信息所必须的易于认知性和唯一识别性,孤立解释上述信息,只会陷入适用僵局。

最后,《个人信息保护法》第28条第1款采取不完全列举,敏感个人信息不限于上述类别,其他类别的个人信息满足敏感风险基准的,亦属于敏感个人信息,如性取向、未公开的违法犯罪记录等,这些信息一旦泄露,不仅侵犯隐私权,且容易引发歧视。[52]

注释:

①我国立法中,《信息安全技术公共及商用服务信息系统个人信息保护指南》《信息安全技术个人信息安全规范》直接对个人敏感信息进行了界定,《征信业管理条例》《App违法违规收集使用个人信息行为认定方法》《自然资源部办公厅关于完善信息平台网络运维环境推进不动产登记信息共享集成有关工作的通知》《国务院办公厅关于促进“互联网+医疗健康”发展的意见》等均体现了个人敏感信息严格保护的理念和规

则。域外立法中,欧盟《通用数据保护条例》第9条明确将种族或民族起源、政治观点、宗教和哲学信仰、工会资格、基因信息和生物信息列举为特殊种类信息;日本《个人信息保护法》第2条第3款将种族、信仰、社会地位、病史、犯罪记录、曾遭受犯罪侵害的事实列为需特殊保护的个人信息。

②采主观基准的观点,参见吴标兵、许和隆:《个人信息的边界、敏感度与中心度研究——基于专家和公众认知的数据分析》,载《南京邮电大学学报(社会科学版)》2018年第5期,第46—51页。

③采客观基准的观点,参见胡文涛:《我国个人敏感信息界定之构想》,载《中国法学》2018年第5期,第241页。兼采主客观基准的观点,参见谢琳、王滢:《我国个人敏感信息的内涵与外延》,载《电子知识产权》2020年第9期,第7—8页。

④参见谢琳、王滢:《我国个人敏感信息的内涵与外延》,载《电子知识产权》2020年第9期,第8—10页;胡文涛:《我国个人敏感信息界定之构想》,载《中国法学》2018年第5期,第249—250页。

⑤参见刘德良:《个人信息保护与中国立法的选择》,载陈海帆、赵国强主编:《个人资料的法律保护:放眼中国内地、香港、澳门及台湾》,社会科学文献出版社2014年版,第44—45页。

⑥参见王晗、秦克飞:《网络用户个人信息的敏感度研究》,载《情报杂志》2012年第12期,第175页。

⑦See Boterberg Sofie & Warreyn Petra, Making Sense of It All: The Impact of Sensory Processing Sensitivity on Daily Functioning of Children, 92 Personality and Individual Differences 80, 85(2016).

⑧“感觉加工敏感”是心理学概念,其是指中枢神经系统具有更强敏感性,对身体、社会和情绪具有更深认知过程的人格特质,拥有感觉加工敏感特质的个人往往更易受到外界刺激并产生正面或者负面反应。See Elaine Aron, The Highly Senitive Person 17(Kensington Publishing Corp. 1996).

⑨日本《个人信息保护法》第2条第3款规定,本法案所称“需要特殊保护的个人信息”是指包括种族、宗教、社会地位、医疗历史、犯罪记录、因犯罪遭受损害的事实,或者其他内阁命令规定的为避免引发歧视、偏见或者其他不利而需要特殊保护的个人信息。从界定和立法意旨来看,“需要特殊保护的个人信息”基本与“敏感个人信息”同义。

⑩参见宁园:《个人信息保护中知情同意规则的坚守与修正》,载《江西财经大学学报》2020年第2期,第117—118页。

⑪我国民法典第1165条第1款规定,行为人因过错侵害他人民事权益造成损害的,应当承担侵权责任。第1167条规定,侵权行为危及他人人身、财产安全的,被侵权人有权请求侵权人承担停止侵害、排除妨碍、消除危险等侵权责任。前者是对已经发生的损害后果的救济,后者则是针对行为虽尚未导致实际损害发生,但正在危及权益时进行的预防性救济。因此,造成实际损害和危及人身、财产安全均属“侵害”范畴。参见黄薇主编:《中华人民共和国民法典侵权责任编释义》,法律出版社2020年版,第12—14页。

⑫如我国民法典第1009条规定“从事与人体基因、人体胚胎等有关的医学和科研活动……不得危害人体健康……”其中的“危害”与侵害同义。除此之外,我国民法典使用“危害”一词的条文还包括:第433条“足以危害质权人权利的,质权人有权请求出质人提供相应的担保”,第534条“对当事人利用合同实施危害国家利益、社会公共利益行为的,市场监督管理和其他有关行政主管部门依照法律、行政法规的规定负责监督处理”,第1071条“非婚生子女享有与婚生子女同等的权利,任何组织或者个人不得加以危害和歧视”,第1095条“未成年人的父母均不具备完全民事行为能力且可能严重危害该未成年人的,该未成年人的监护人可以将其送养”。

⑬参见《信息安全技术个人信息安全规范》第3.2条。

⑭我国民法典第1032条第2款规定,隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。第1034条第3款规定,个人信息中的私密信息,适用有关隐私权的规定;没有规定的,适用有关个人信息保护的规定。

⑮参见张璐:《何为私密信息?——基于〈民法典〉隐私权与个人信息保护交叉部分的探讨》,载《甘肃政法大学学报》2021年第1期,第93页。

⑯参见许可、孙铭溪:《个人私密信息的再厘清——从隐私和个人信息的关系切入》,载《中国应用法学》2021年第1期,第14页。

⑰参见程啸:《个人信息保护中的敏感信息与私密信息》,载《人民法院报》2020年11月19日,第5版。

⑱参见刘洪岩、唐林:《基于“可识别性”风险的个人信息法律分类——以欧美个人信息立法比较为视角》,载《上海政法学院学报》2020年第5期,第31页;董悦:《公民个人信息分类保护的刑法模式构建》,载《大连理工大学学报(社会科学

版)》2020年第2期,第82—83页。

⑲参见田野、张晨辉:《论敏感个人信息的法律保护》,载《河南社会科学》2019年第5期,第45页。

⑳参见高富平:《2012年〈个人数据处理中的个人保护公约〉评析》,载高富平主编:《个人数据保护和利用国际规则:源流与趋势》,法律出版社2016年版,第65页。

㉑参见张恩典:《反算法歧视:理论反思与制度建构》,载《华中科技大学(社会科学版)》2020年第5期,第62—63页。See Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 Stanford Law Review 1373, 1376(2000).

㉒根据中国信息通信研究院发布的《新形势下电信网络诈骗治理研究报告(2020年)》,2020年1月至10月,信息通信行业累积处置涉诈网络资源15.3亿次,其中诈骗呼叫2.3亿次,诈骗短信13亿余条。参见中国信息通信研究院:《新形势下电信网络诈骗治理研究报告(2020年)》,载中国信通院网,http://www.caict.ac.cn/kxyj/qwfb/ztbg/202012/t20201218_366375.htm,访问时间:2021年3月5日。

㉓参见黄薇主编:《中华人民共和国民法典侵权责任编释义》,法律出版社2020年版,第21—25页;朱晓峰:《论一般人格权条款与具体人格权条款的规范适用关系》,载《比较法研究》2021年第4期,第156页。

㉔参见[美]迈克尔·罗森:《尊严:历史和意义》,法律出版社2015年版,第6页。

㉕《个人信息保护法(草案二审稿)》第29条第2款规定的风险程度为"可能受到歧视或人身、财产安全受到严重危害",其对歧视采一般侵害程度+无差别风险概率(存在可能性即可、与非敏感个人信息的风险兑现概率无差别),对人身、财产安全采严重侵害程度(要求严重危害人身、财产安全)+无差别风险概率。此种区分标准缺乏根据,也不符合权利平等保护的理念,《个人信息保护法》第28条第1款改采统一标准,值得肯定。

㉖参见中国审判理论研究会民事审判理论专业委员会主编:《民法典侵权编条文理解与司法适用》,法律出版社2020年版,第96页。

㉗《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第5条。

㉘我国亦有学者持此观点,将敏感个人信息权益侵害风险表述为"非常大"。参见胡文涛:《我国个人敏感信息界定之构想》,载《中国法学》2018年第5期,第250页。

㉙参见汤敏:《个人敏感信息保护的欧美经验及其启示》,载《图书馆建设》2018第2期,第45页;陈红旭:《敏感个人数据的特殊保护》,载《重庆理工大学学报(自然科学版)》2019年第4期,第119—121页。

㉚See Helen Nissenbaum, Privacy as Contextual Integrity, 79 Washington Law Review 101, 137(2004).

㉛参见胡凌:《个人私密信息如何转化为公共信息》,载《探索与争鸣》2020年第11期,第29页。

㉜理论上,穷尽场景的归纳法亦可以实现敏感个人信息的场景隔离,但归纳法显然不具有可操作性,个人信息处理场景烦琐多变,穷尽难以实现,归纳亦不可能。

㉝参见宁园:《个人信息保护中知情同意规则的坚守与修正》,载《江西财经大学学报》2020年第2期,第117—118页。

㉞参见欧盟《通用数据保护条例》第9条,日本《个人信息保护法》第17条,《信息安全技术个人信息安全规范》第5.4、6.3、9.2、9.4条,《个人信息保护法》第28—32条。

㉟基因序列是使用一串字母表示的真实的或者假设的携带基因信息的DNA分子的一级结构。DNA由四种脱氧核苷酸链接而成的,这四种脱氧核苷酸分别简称A、T、G、C,四种脱氧核苷酸的排列组合就构成了基因序列。专业认为可通过基因测序分析测定基因序列,预测罹患多种疾病(如癌症或白血病)的可能性。

㊱参见肖峰:《重勘信息的哲学含义》,载《中国社会科学》2010年第4期,第34—38页。

㊲本文采信息认识论,认为信息以主体认识为先决条件,不存在不被认识的、先于主体存在的信息。有关信息本体论和信息认识论的争议,信息哲学领域尚无定论。相关争议,参见邬焜:《中国信息哲学核心理论的五种范式》,载《自然辩证法研究》2011年第4期,第48—53页。

㊳参见[英]卢西亚诺·弗洛里迪:《图灵的三个哲学教益与信息哲学》,姜晨程译,《哲学分析》2020年第1期,第135页。

㊴参见[英]维纳:《人有人的用处——控制论与社会》,陈步译,北京大学出版社2010年版,第13—20页。

㊵参见王亮:《论信息的中介普遍性》,载《西安交通大学学报(社会科学版)》2015年第6期,第91页。

㊶有关描述性信息这一类型的讨论,参见李怡:《个人一般信息侵权裁判规则研究——基于68个案例样本的类型化分析》,载《政治与法律》2019年第9期,第151页。

㊷MAC地址即媒体存取控制位置,是用来确认网络终端

设备位置的地址，一台终端设备的一个网卡对应唯一的MAC地址。MAC地址可以作为区分设备使用主体身份的工具，具有直接识别性，但多人使用一台设备的情形下，MAC地址对应多个设备使用主体，因而不具有唯一性。

㊸本文认为，个人信息在歧视和其他人身、财产权利侵害中的作用形式不同，歧视是偏见的外化，信息仅需暴露于个人并由其接收，即可能刺激偏见产生，进而有可能外化为歧视；其他人身、财产权利侵害则须以信息为工具，是认识信息且利用信息的过程。

㊹此处的权力是指强势一方拥有可以贯彻自己意志而不顾弱势一方反对的任何机会。参见[德]马克思·韦伯：《经济与社会》(下卷)，林荣远译，商务印书馆2006年版，第81页。

㊺参见黄家亮：《论社会歧视及其治理——一个社会学视角的理论分析》，载《华东理工大学学报(社会科学版)》2008年第3期，第2页。

㊻参见北京市第一中级人民法院(2017)京01民终509号民事判决书。

㊼《个人信息保护法》第73条将自动化决策界定为“通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动”。

㊽参见林洹民：《个人对抗商业自动决策算法的私权设计》，载《清华法学》2020年第4期，第125—126页。

㊾《个人信息保护法》第24条对自动化决策场景下的个人信息处理作了专门规定，第55条要求利用自动化决策处理个人信息的须先进行个人信息保护影响评估。

㊿《个人信息保护法》第62条亦规定，国家网信部门统筹协调有关部门推进针对人脸识别、人工智能等新技术、新应用的专门立法工作。

(51)有关各列举项所包含的具体个人信息内容，可参见《信息安全技术个人信息安全规范》附录A、附录B。

(52)其他类型的敏感个人信息可参见《信息安全技术个人信息安全规范》附录B。

The Legal Attributes and Definition of Sensitive Personal Information: Centered on the First Paragraph of Article 28 of Personal Information Protection Law of PRC

Ning Yuan

Abstract: The sensitivity of sensitive personal information refers to the high responsiveness regulated by law, which is measured by the risk of infringement of rights in the processing information. Its definition should take a dual path of de-contextualization and contextualization. Its scope shall be defined by referring on the one hand to the de-contextualized information content itself, and on the other hand to the external factors that constitute the elements of the scene in the context, for the general personal information can be transformed into sensitive ones when it is contextualized to produce strong instrumentality and unique identification.

Key words: sensitive personal information; risk dimensions; contextual segregation; contextual integration; strong instrumentality; unique identification